



DEPARTMENT OF THE ARMY

U.S. Army Corps of Engineers
WASHINGTON, D.C. 20314-1000

REPLY TO
ATTENTION OF:

CEPM (380-19)

10 February 1995

MEMORANDUM FOR DIRECTORS, HQUSACE
CHIEFS, SEPARATE OFFICES
COMMANDERS, USACE COMMANDS

SUBJECT: Automated Information Systems Security Incident and Technical Vulnerability
Reporting Policy and Procedures

1. References;

- a. AR 380-19, Information Systems Security, 1 Aug 90.
- b. AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA), 15 Jan 93.

2. Subject reports are required by para 2-28 add 2-29 of ref a and para 3-4a of ref b. This memorandum provides USACE policy and procedures for reporting all automated information systems security incidents and technical vulnerabilities reporting.

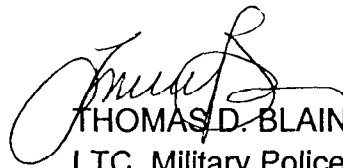
3. Upon receipt of this memorandum all AIS incidents and technical vulnerabilities, to include virus infections, hacker attacks, and computer security violations, will be reported to the USACE ISSPM via electronic mail within 24 hours of the occurrence. The report will consist of a brief statement containing the location affected, system affected, a description of the suspected or confirmed incident, action taken, and point of contact. If the incident is a virus infection, also include a list of all possible contacts with the infected computer or infected computer disk. Notification should be sent to all contacts of the possibility of virus infection.

4. USACE Policy is to report suspected or actual AIS security incidents to the appropriate ISSO, who will notify the ISSM and initiate an investigation. The ISSM will forward the initial report to the USACE ISSPM and initiate a preliminary inquiry under AR 380-5 and AR 380-6, if appropriate. All incidents that indicate foreign intelligence involvement will be reported in accordance with AR 381-12. Initial report will be to the USACE ISSPM, who will advise if further action must be taken.

5. If needed, a final report of a confirmed AIS security incident will be sent through Headquarters, US Army Corps of Engineers, Attn: CEPM-ZC, 20 Massachusetts Ave NW, Washington, DC 20314-1000, to Defense Information Systems Agency (DISA), Center for Information Systems Security (CISS), 5113 Leesburg Pike, Suite 400, Falls Church, VA 22041-3230, within 60 days from the discovery of the incident. Information copies of the report will be provided for HQDA (DAMI-CIP and SAIS-C4C). The full report will contain all relative documentation, including the corrective action taken. This report should be in sufficient detail so that DISA analyst can demonstrate and repeat the vulnerability.

6. Questions and/or guidance request on this policy should be directed to Mr. Thomas J. Aubin, CEPM-ZC, (202) 272-8723.

FOR THE COMMANDER



THOMAS D. BLAIN
LTC, Military Police
Chief, Security and Law
Enforcement